СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

Алгоритм Диффи-Хэлман

Алгоритм Диффи-Хеллмана (Diffie-Hellman algorithm) – это криптографический алгоритм, позволяющий двум сторонам установить общий секретный ключ, используя незащищенный канал связи. Этот алгоритм был предложен в 1976 году Уитфилдом Диффи и Мартом Хеллманом и стал основой для разработки методов шифрования с открытым ключом. Через год после изобретения алгоритма Диффи-Хеллмана был создан первый алгоритм асимметричного шифрования RSA, который позволил решить проблему общения через незащищенный канал, больше не требуя от каждой стороны наличия копии одного и того же секретного ключа.

Описание алгоритма

Две стороны (Алина и Борис) хотят установить общий секретный ключ для последующего использования в шифровании. Для этого они используют незащищенный канал связи.

1) Алина и Борис выбирают два больших простых числа p и g, а также свои секретные ключи a и b соответственно.

Алина вычисляет значение A и передает Борису:

$$\mathrm{A} = g^{a} \, mod \, p. \tag{6}$$

Борис Вычисляет значение B и передает Алине:

$$B = g^{b} \, mod \, p. \tag{7}$$

2) Получение общего секретного ключа

Алина получает значение B и вычисляет значение К:

$$\mathrm{К} = B^{a} \, mod \, p = g^{ab} \, mod \, p. \tag{8}$$

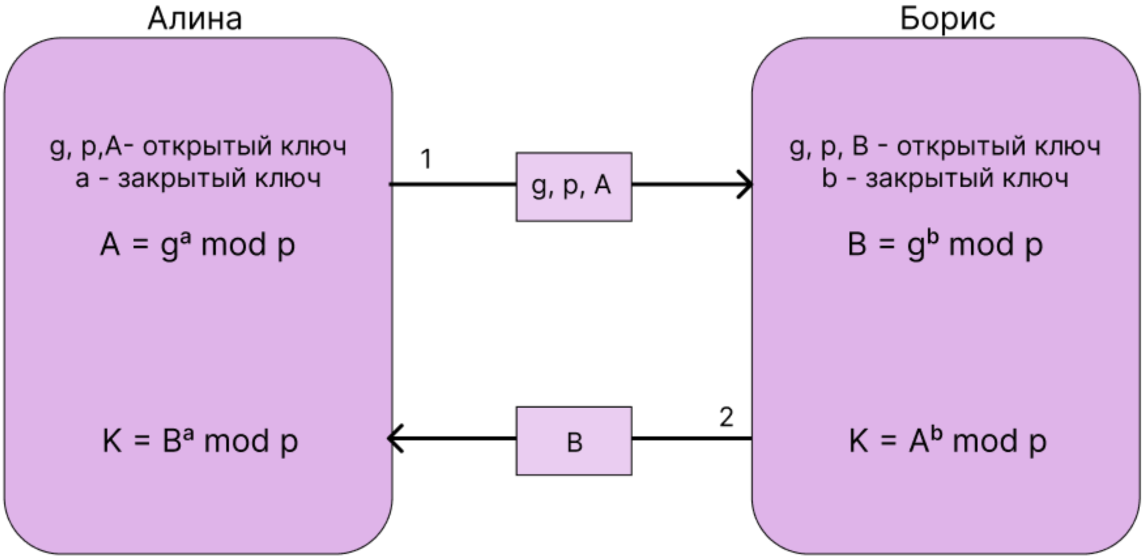
Борис получает значение A и вычисляет значение К:

$$\mathrm{К} = \mathrm{A}^{b} \, mod \, p = g^{ab} \, mod \, p. \tag{9}$$

Алина и Борис в качестве секретного ключа могут использовать К=$g^{ab} \, mod \, p$.

Злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления $g^{ab} \, mod \, p$ по перехваченным $g^{a} \, mod \, p$ и $g^{b} \, mod \, p$, если числа p,a,b выбраны достаточно большими.

В практических реализациях для a и b используются числа порядка 10^{100} и для p - порядка 10^{300}. Число g необязательно должно быть большим и обычно имеет значение в пределах первого десятка.



$$K = A^b \bmod p = (g^a \bmod p)^b = g^{ab} \bmod p = (g^b \bmod p)^a = B^a \bmod p$$

Рисунок 26. Схема алгоритма Диффи-Хеллмана

Использование алгоритма Диффи - Хеллмана не ограничено только двумя участниками. Оно может быть применено к любому количеству пользователей. Давайте рассмотрим ситуацию, когда Алиса, Боб и Кэрол совместно генерируют исходный ключ. Последовательность действий в этом случае будет следующей:

1) участники выбирают числа p и g;

2) участники, Алина, Борис и Катя генерируют свои ключи — a, b и c соответственно;

3) Алина вычисляет g^a mod p и отправляет его Борису;

4) Борис вычисляет $(g^a)^b$ mod p = g^{ab} mod p и отправляет его Кате;

5) Катя вычисляет $(g^{ab})^c$ mod p = g^{abc} mod p и получает тем самым общий секретный ключ;

6) Борис вычисляет g^b mod p и отправляет его Кате;

7) Катя вычисляет $(g^b)^c$ mod p = g^{bc} mod p и отправляет его Алине;

8) Алина вычисляет $(g^{bc})^a$ mod p = g^{bca} mod p = g^{abc} mod p — общий секретный ключ;

9) Катя вычисляет g^c mod p и отправляет его Алине;

10) Алина вычисляет $(g^c)^a$ mod p = g^{ca} mod p и отправляет его Борису;

11) Борис вычисляет $(g^{ca})^b$ mod p = g^{cab} mod p = g^{abc} mod p и также получает общий секретный ключ.

Если злоумышленник будет прослушивать канал связи, то он сможет узнать значения g^a mod p, g^b mod p, g^c mod p, g^{ab} mod p, g^{ac} mod p, и g^{bc} mod p, но при этом не сможет получить g^{abc} mod p используя любые комбинации этих чисел.

Задача: Вычислить открытые ключи А, В и секретный ключ К при выполнении алгоритма Диффи-Хеллмана.

Вариант 1

g, p	13, 7
a, b	5, 4

Вариант 2

g, p	15, 11
a, b	6, 8

Вариант 3

g, p	11, 3
a, b	7, 6

Вариант 4

g, p	4, 15
a, b	3, 8

Вариант 5

g, p	6, 13
a, b	4, 7

Вариант 6

g, p	7, 12
a, b	3, 2

Вариант 7

g, p	5, 14
a, b	6, 4

Вариант 8

g, p	11, 13
a, b	3, 7

Вариант 9

g, p	9, 16
a, b	4, 11

Вариант 10

g, p	7, 11
a, b	6, 13

Криптографический алгоритм RSA

RSA – криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности). Криптосистема RSA разработана в 1977 году и названа в честь ее разработчиков Ronald Rivest, Adi Shamir и Leonard Adleman. Алгоритм RSA работает следующим образом: берутся два достаточно больших простых числа p и q и вычисляется их произведение n = p*q; n называется модулем. Затем выбирается число e, удовлетворяющее условию 1< e < (p - 1)*(q - 1) и не имеющее общих делителей кроме 1 (взаимно простое) с числом (p - 1)*(q - 1). Затем вычисляется число d таким образом, что (e*d - 1) делится на (p - 1)*(q – 1).

- e – открытый (public) показатель;
- d – частный (private) показатель;
- (n; e) – открытый (public) ключ;
- (n; d). – частный (private) ключ.

Делители (факторы) p и q можно либо уничтожить либо сохранить вместе с частным (private) ключом.

Если бы существовали эффективные методы разложения на сомножители (факторинга), то, разложив n на сомножители (факторы) p и q, можно было бы получить частный (private) ключ d. Таким образом надежность криптосистемы RSA основана на трудноразрешимой – практически неразрешимой – задаче разложения n на сомножители (то есть на невозможности факторинга n) так как в настоящее время эффективного способа поиска сомножителей не существует.

Ниже описывается использование системы RSA для шифрования информации и создания цифровых подписей (практическое применение немного отличается).

Криптосистема Эль-гамаль

Схема Эль-Гамаля – криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Схема была предложена Тахером Эль-Гамалем в 1985 году. Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. Схема шифрования Эль-Гамаля представлена на рис. 27:

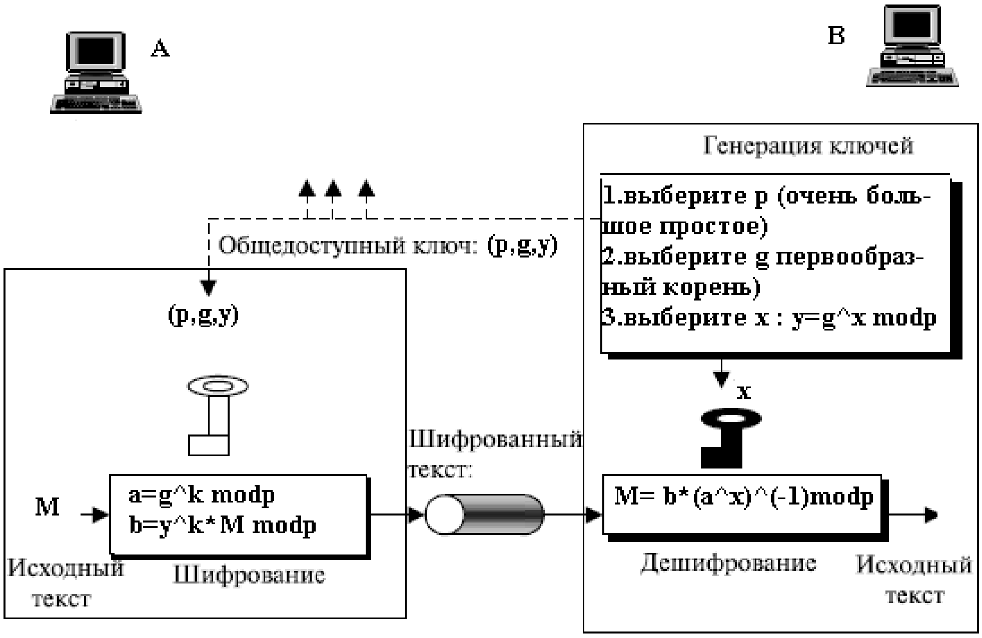


Рисунок 27. Схема шифрования алгоритма Эль-Гамаля

Шифрование

Сообщение M должно быть меньше числа p. Сообщение шифруется следующим образом:

1) Выбираются числа p, g и x, такие что:

- p простое, p>M;
- g – первообразный корень p;
- x – случайное целое число, 1<x<p.

2) Вычисляется $y = g^x \; mod \; p$;

3) Формируется открытый ключ (p,g,y), x – закрытый ключ;

4) Выбирается сессионный ключ — случайное целое число, взаимно простое с (p-1), k такое, что 1<k<p-1;

5) Вычисляются числа $a = g^k \; mod \; p$ и $b = y^k M \; mod \; p$;

6) Пара чисел (a,b) является шифротекстом.

Нетрудно заметить, что длина шифротекста в схеме Эль-Гамаля вдвое больше исходного сообщения M.

Расшифрование

Зная закрытый ключ x, исходное сообщение можно вычислить из шифротекста (a,b) по формуле: $M = b(a^x)^{-1}\ mod\ p$

При этом нетрудно проверить, что $(a^x)^{-1} = g^{-kx}\ mod\ p$

и поэтому $b(a^x)^{-1} = (My^x)g^{-xk} \equiv (Mg^{xk})g^{-xk} \equiv M\ mod\ p$

Для практических вычислений больше подходит следующая формула:

$$M = b(a^x)^{-1}\ mod\ p.$$

Пример

Шифрование

Необходимо зашифровать сообщение M=4.

1) генерация ключей:

– пусть p=11, g=2, x=9;

– $y = g^x\ mod\ p = 2^9\ mod\ 11 = 6$

(11,2,6) – открытый ключ, x=9 – закрытый ключ

2) пусть k=7 – закрытый ключ

3) $a = g^k\ mod\ p = 2^7\ mod\ 11 = 7$

4) $b = y^k M\ mod\ p = 6^7 4\ mod\ 11 = 10$

(a,b) = (7,10) – зашифрованное сообщение

Расшифрование

Необходимо получить сообщение M=4 по зашифрованному сообщению (a,b) = (7,10) и закрытому ключу x=9.

$$M = b(a^x)^{-1}\ mod\ p = 10(7^9)^{-1}\ mod\ 11 = 4.$$

Задача: Зашифровать сообщение, определить значение y и выполнить проверку(расшифровать).

Вариант 1

Сообщение, M	10
Открытый ключ, (p, g)	(17,7)
Закрытый ключ, (x, k)	(11, 13)

Вариант 2

Сообщение, M	13
Открытый ключ, (p, g)	(23,7)
Закрытый ключ, (x, k)	(10, 6)

Вариант 3

Сообщение, M	6
Открытый ключ, (p, g)	(13,2)
Закрытый ключ, (x, k)	(7, 10)

Вариант 4

Сообщение, M	8
Открытый ключ, (p, g)	(17,5)
Закрытый ключ, (x, k)	(6, 9)

Вариант 5

Сообщение, M	5
Открытый ключ, (p, g)	(11,8)
Закрытый ключ, (x, k)	(6, 6)

Вариант 6

Сообщение, M	4
Открытый ключ, (p, g)	(11,5)
Закрытый ключ, (x, k)	(5, 7)

Вариант 7

Сообщение, M	9
Открытый ключ, (p, g)	(13,7)
Закрытый ключ, (x, k)	(4, 3)

Вариант 8

Сообщение, M	7
Открытый ключ, (p, g)	(3,4)
Закрытый ключ, (x, k)	(5, 6)

Вариант 9

Сообщение, M	10
Открытый ключ, (p, g)	(7,3)
Закрытый ключ, (x, k)	(5, 5)

Вариант 10

Сообщение, M	7
Открытый ключ, (p, g)	(8,3)
Закрытый ключ, (x, k)	(6, 3)